CLAIMS

1. A method in a computing system for updating properties used by a subject computer system using a helper computer system, comprising:

maintaining a set of current properties on the subject computer system;

in the helper computer system, receiving new properties for the subject computer system;

transmitting the current properties from the subject computer system to the helper computer system;

in the helper computer system,

merging the received new properties into a copy of the transmitted current properties;

comparing the received current properties to the copy of the received current properties into which were merged the received new properties;

if the received current properties to the copy of the received current properties differ, transmitting the copy of the current properties into which were merged the received new properties to the subject computer system; and

in the subject computer system, adopting the transmitted copy of the current properties into which were merged the received new properties.

2. The method of claim 1 wherein the comparing includes:

generating a digest of each the received current properties to the copy of the received current properties into which were merged the received new properties; and

comparing the generated digests.

3. The method of claim 2 wherein the digests are generated using a hashing function.

4. The method of claim 2 wherein the digests are generated using an MD5 hashing function.

5. The method of claim 2 wherein the merging includes:

deleting from the copy of the current properties any properties managed by the helper computer system; and

adding properties including the new properties to the copy of the current properties.

6. The method of claim 5 wherein the deleting includes deleting properties in the copy of the current properties identified by administrative properties among the current properties.

7. The method of claim 1 wherein the merging includes adding to the copy of the current properties administrative properties identifying other properties added to the copy of the current properties.

8. A method in a computing system for remotely managing properties for a subject computer system, comprising:

receiving a property update inquiry from the subject computer system, the inquiry indicating a time at which properties in use by the subject computer system were updated;

comparing the indicated time to an update time for managed properties;

if the indicated time is earlier than the update time,

retrieving a copy of the existing properties used by the subject computer system;

merging managed properties into the copy of the existing properties; and

sending the merged properties to the subject computer system.

9. The method of claim 8 wherein the merged properties sent to the subject computer system include an instruction to adopt the merged properties.

10. The method of claim 8, further comprising comparing the merged properties to the existing properties, and wherein the sending is only performed if the merged properties and the existing properties are not the same.

11. A method in a server computer system for establishing a virtual private network between a first private network having a first security device and a second private network having a second security device, comprising:

generating properties for the first security device to direct the participation of the first security device in the virtual private network;

generating properties for the second security device to direct the participation of the second security device in the virtual private network;

distributing the properties generated for the first security device to the first security device for use by the first security device to participate in the virtual private network; and

distributing the properties generated for the second security device to the second security device for use by the second security device to participate in the virtual private network.

12. The method of claim 11 wherein the properties generated for the first security device are distinct from the properties generated for the second security device.

13. The method of claim 11 wherein the generated properties are adopted by both security devices to establish the virtual private network.

14. The method of claim 11 wherein the distributing includes transmitting the generated properties to the security devices in response to inquiries from the security devices at times subsequent to the generating.

15. The method of claim 11 wherein the distributing includes transmitting the generated properties to the security devices in response to the generation of the properties.

16. The method of claim 11, further comprising receiving a single set of VPN specifications in the server computer system,

and wherein the method is performed without regard for any user input received subsequent to receiving the single set of VPN specifications.

17. The method of claim 11 wherein the generation of properties for each security device includes:

selecting a property template; and

populating the selected property template with information specific to the first private network and/or information specific to the second private network.

18. The method of claim 11 wherein the generated properties include security properties relating to the protection of data traveling in the virtual private network.

19. The method of claim 18 wherein the security properties specify encryption parameters for data traveling in the virtual private network.

20. The method of claim 11 wherein the generated properties include resource properties relating to sources and destinations in the private networks for data traveling in the virtual private network.

21. The method of claim 20 wherein the resource properties specify addresses of network nodes within the private networks that may send and receive data traveling in the virtual private network.

22. The method of claim 11 wherein the generated properties include service properties relating to classes of data that may travel in the virtual private network.

23. The method of claim 22 wherein the service properties specify network protocols for which data may travel in the virtual private network.

24. The method of claim 11, further comprising performing the generating and distributing for one or more additional security devices in order to establish the virtual private network between more than two private networks.

25. A computer-readable medium whose contents cause a server computer system to establish a virtual private network between a first private network having a first security device and a second private network having a second security device by:

generating properties for the first security device to direct the participation of the first security device in the virtual private network;

generating properties for the second security device to direct the participation of the second security device in the virtual private network;

distributing the properties generated for the first security device to the first security device for use by the first security device to participate in the virtual private network; and

distributing the properties generated for the second security device to the second security device for use by the second security device to participate in the virtual private network.

26. A single memory containing a data structure usable to establish a virtual private network between a first private network and a second private network, comprising:

properties usable by a security device of the first private network to establish the virtual private network; and

properties usable by a security device of the second private network to establish the virtual private network.

27. The memory of claim 26 wherein the memory is connected to a computer system that has a supervisory relationship with both the security device of the first private network and the security device of the second private network.

28. A method in a single manager computing system for managing properties for a plurality of managed computer systems, comprising, reiteratively:

receiving new managed properties for an identified managed computer system; and

delivering the received new managed properties to the identified managed computer system.

29. The method of claim 28 wherein at least one of the managed computer systems is a dedicated network security device.

30. The method of claim 28 wherein, for each managed computer system, the managed properties are a proper subset of a set properties used by the managed computer system, and wherein the delivering includes:

receiving the set of properties used by the managed computer system;

substituting for managed properties in the set of properties used by the managed computer system new managed properties received by the manager computer system; and

conveying to the managed computer system the set of properties used by the managed computer system in which the new managed properties have been substituted.

31. The method of claim 28, further comprising cacheing the received new managed properties until delivery.

32. The method of claim 28, further comprising determining whether the new managed properties received differ from those in use by the identified managed computer system,

and wherein the new managed properties are delivered only if it is not determined that the new managed properties received differ from those in use by the identified managed computer system.

33. A manager computing system for managing properties for a plurality of managed computer systems, comprising:

a receiving subsystem that receives new managed property sets, each for an identified managed computer system; and

a delivery subsystem that delivers new managed property sets received by the receiving subsystem each to the identified managed computer system.

34. A method in a distinguished computing system for managing properties used by the distinguished computer system in its operation, comprising:

maintaining a first set of properties;

receiving from a separate computing system a second set of properties; and

using both the first set of properties and the second set of properties in the operation of the distinguished computing system.

35. The method of claim 34, further comprising:

updating one or more properties among the first set of properties at the initiation of the distinguished computing system; and

using the updated properties in the operation of the distinguished computing system.

36. The method of claim 34, further comprising:

receiving one or more updated properties from the separate computing system; and

using the updated properties in the operation of the distinguished computing system.

37. The method of claim 36 wherein the updated properties specify the establishment of a virtual private network between the distinguished computing system and an additional computing system.

38. The method of claim 34, further comprising:

sending the first and second sets of properties as a configuration to the separate computing system;

receiving from the separate computer system a replacement configuration, in which properties of the second set have been modified; and

using the properties in the replacement configuration in the operation of the distinguished computing system.

39. A method in a manager computing system for participating in the management of properties used by a client computing system, comprising:

determining that properties of the client computing system managed by the manager computing system should be updated; and

instructing the client computing system to use in its operation manager-managed properties updated in accordance with the determination, in conjunction with properties of the client computing system managed by the client computing system.

40. The method of claim 39, further comprising:

receiving from the client computing system a client configuration comprising the manager-managed properties and client-managed properties in use by the client computing system;

incorporating in the received client configuration the manager-managed properties updated in accordance with the determination to produce an updated client configuration; and

returning the updated client configuration to the client computing system with an instruction to use the updated client configuration in the operation of the client computing system.

41. The method of claim 39 wherein the updated properties specify the establishment of a virtual private network between the client computing system and an additional computing system.

42. A system for managing properties for a distinguished computing system, comprising:

the distinguished computing system, which utilizes both locally-managed properties and remotely-managed properties, and which manages the locally-managed properties; and

a manager computing system communicatively connected to the distinguished computing system, which manages the remotely-managed properties.

43. The method of claim 42 wherein the distinguished computing system is a specialized network security device.